# DORA im Rampenlicht: Die Integration des EU-Rahmenwerks in Ihr Compliance-Ökosystem

Im Zuge der weltweit fortschreitenden digitalen Transformation wurde Finanzunternehmen in der Europäischen Union das Management digitaler Betriebsrisiken und Resilienz dem eigenen Ermessen überlassen. Der von der Europäischen Kommission im September 2020 vorgestellte Digital Operational Resilience Act (DORA) zielt darauf ab, einen einheitlichen Rahmen für das Management und die Minderung von Risiken der Informations- und Kommunikationstechnologie (IKT) auf EU-Ebene zu schaffen. DORA wurde im November 2022 verabschiedet und trat im Januar 2023 offiziell in Kraft. Ab dem 17. Januar 2025 findet DORA Anwendung – bis dahin müssen alle Finanzinstitute in der EU konform sein.

## Verständnis des regulatorischen Umfangs von DORA

Angesichts des digitalen und vernetzten Charakters des heutigen Finanzökosystems müssen viele Unternehmen, die bisher nicht den Vorschriften an die IT- und Informationssicherheit (u.a. BAIT, VAIT) unterlagen, nun die DORA-Vorschriften einhalten. Das Regelwerk listet 21 spezifische Arten von Unternehmen, darunter nicht nur traditionelle Finanzunternehmen wie Kredit- und Zahlungsinstitute und Investmentfirmen, sondern auch IKT-Drittdienstleister wie Cloud-Service-Anbieter und Rechenzentren. Außerdem hebt sich DORA von anderen Vorschriften durch seinen Schwerpunkt auf IKT ab, was eine bedeutende regulatorische Veränderung für alle Finanzinstitute darstellt. Zu den spezifischen Anforderungen von DORA gehören:

– Fokus auf die Aufrechterhaltung des Kundenzugangs zu wichtigen, digitalen Diensten
– Angepasste Risikomethode, die die Durchführung einer Analyse der Auswirkungen auf den Geschäftsbetrieb erfordert, wobei die potenziellen Auswirkungen schwerwiegender Geschäftsunterbrechungen anhand quantitativer und qualitativer Kriterien bewertet werden
– Verantwortlichkeit für alle nachgelagerten Risiken im erweiterten Netzwerk eines Finanzunternehmens – dieser breitere Geltungsbereich umfasst die Durchführung von Risikobewertungen, Due-Diligence-Prüfungen und das Risikomanagement für traditionelle Dritte, Vierte und letztlich N-te Parteien über direkte und indirekte oder untervergebene Lieferkettenpartner
– Erfordernis, alle Personen, Informations- und IKT-Applikationen sowie die Verbindungen, Funktionen und Abhängigkeiten zwischen ihnen zu identifizieren und detailliert in einem Informationsregister zu erfassen (Artikel 28), wobei keine Verträge mit IKT-Drittanbietern geschlossen werden dürfen, die nicht nachweisen können, dass sie DORA-konform sind
– Meldung größerer Cyber-Vorfälle an eine zuständige nationale Behörde zur Streuung der Nachricht, sowie eine zentralisierte Prüfung kritischer Drittparteien

DORA enthält jedoch einen Grundsatz der Verhältnismäßigkeit (Artikel 4), der es Finanzunternehmen mit einer bestimmten Größe und Risikoprofil ermöglicht, weniger strenge Anforderungen zu erfüllen. Die Regulierung sieht auch ein vereinfachtes Rahmenwerk für das IKT-Risikomanagement (Artikel 16) vor, bei dem bestimmte kleine und nicht miteinander verbundene Finanzunternehmen von den Hauptanforderungen ausgenommen werden können.

## Integration von DORA mit OneTrust

Das Finanzwesen ist einer der am stärksten regulierten Sektoren. Die Einhaltung von DORA, neben zahlreichen anderen Rahmenwerken und Vorschriften, kann zu doppelten Anstrengungen, überlasteten Ressourcen und Prüfungsmüdigkeit führen.

OneTrust erleichtert die Integration von DORA in umfassendere Regulierungs- und Cybersicherheitsrahmenwerke, indem es Bereiche mit Überschneidungen identifiziert und gemeinsame Kontrollen nutzt. Mit automatisierten Integrationen und Workflows rationalisiert die Plattform die Richtlinien, Verfahren und Kontrollen des Risikomanagements. Ein konsolidiertes Dashboard und Echtzeitwarnungen liefern aktuelle Informationen über Ihre Sicherheitslage, sodass Sie Anomalien oder Mängel noch vor der Prüfung beheben können.

Darüber hinaus bietet OneTrust angesichts der in DORA enthaltenen Anforderungen an das Risiko von Drittanbietern Bewertungen von Drittanbietern und anpassbare Vorlagen. Drittparteien werden geprüft und mithilfe datengesteuerter Automatisierungsworkflows kontinuierlich auf Änderungen überwacht. Weiterhin unterstützt OneTrust Sie dabei, ein Informationsregister aufzubauen, indem sie durch intelligente Fragebögen Informationen zu Ihren IKT-Services auf verschiedenen Ebenen abfragen können.

*Autor: Katrina Dalao, Senior Content Marketing Specialist (CIPM, CIPP/E) @ OneTrust*

Weitere Informationen darüber, wie OneTrust dabei helfen kann, die DORA-Anforderungen zu erfüllen und die digitale betriebliche Resilienz in einer sich ständig verändernden Cyberlandschaft aufrechtzuerhalten, erhalten Sie in unserem Webinar in Partnerschaft mit PwC am 6. Februar 2024.